COMPARECENCIA ANTE LA COMISIÓN CONSTITUCIONAL DEL CONGRESO DE LOS DIPUTADOS. MEMORIA 2008

(17- Mayo - 2009)

Señor Presidente, Señorías,
Buenas tardes,

Comparezco ante esta Comisión Constitucional para dar cuenta de la Memoria de la Agencia Española de Protección de datos correspondiente al año 2008.

Con el fin de que sus Señorías puedan tener una visión integral sobre el estado de situación de la protección de datos, haré referencia en primer lugar, a los temas más destacables de la Memoria para informar, a continuación, sobre problemas más recientes de la protección de datos en nuestro país.

Comenzaré mi intervención afirmando, una vez más, que la prioridad de la Agencia son los derechos de los ciudadanos. Por ello consideramos imprescindible impulsar la información de forma que los ciudadanos sean cada vez más conscientes de los derechos sobre sus datos personales y así hacerlos efectivos.

Para conseguir que los ciudadanos puedan tener más información, la Agencia ha impulsado dos canales prioritarios:

- Un Servicio de Atención al Ciudadano que facilita información presencial, telefónica y por escrito a las consultas que se nos plantean.
- Y la difusión, a través de los medios de comunicación, de los riesgos más relevantes que afectan a la protección de datos personales.

La Memoria de 2008 constata un incremento de más del 50% de las consultas.

Los principales temas objeto de consulta persiguen:

1º) Evitar la recepción de publicidad, fundamentalmente telefónica, bien a través de llamadas o de la recepción de mensajes SMS.

2º) Resolver dudas sobre los ficheros de morosos relativas la legalidad de la inclusión en los mismos y a las empresas de recobro de deudas.

3º) A estas dudas se añaden las referidas a la historia clínica y a la negativa a facilitar información sobre las mismas.

En 2008 la Agencia ha tratado de medir el nivel de satisfacción de los ciudadanos sobre este canal de información y hemos constatado:

- que la mitad de los ciudadanos tenían ya conocimiento de la materia antes de consultar a la Agencia.

- y que la información facilitada les resultaba satisfactoria.

Con ello, concluimos, con satisfacción, que avanzamos en el objetivo de conseguir una Agencia más abierta y útil para los ciudadanos.

A ello contribuye, sin duda, la profesionalidad y sensibilidad que demuestran los funcionarios al servicio de la Agencia.

En cuanto a la promoción de la difusión a través de los medios de comunicación, permítanme unos breves indicadores:

- En 2008, se han duplicado las entrevistas y demandas de información a la Agencia, tanto en medios de información general como especializada, ya audiovisuales, radiofónicos o escritos.

- La mayor sensibilidad de los medios de comunicación nos ha permitido conocer en mayor medida incumplimientos de la normativa de protección de datos que, por la alarma social que han suscitado, han propiciado investigaciones de oficio.

- La información difundida ha permitido focalizar las cuestiones que son más sensibles para el publico (videovigilancia, documentación abandonada en la vía pública, filtración de datos sensibles a través de redes de intercambio de archivos en Internet, o las redes sociales).

Quiero agradecer, por ello, a los medios de comunicación su contribución al objetivo de que los ciudadanos conozcan mejor sus derechos y los puedan ejercer.

Lo cierto es que la concienciación ciudadana en España en materia de protección de datos personales se sitúa claramente por encima de la media comunitaria.

Y, en particular, su principal inquietud reside en saber cómo ejercer sus derechos. No en vano, cerca de un tercio de las consultas recibidas por la Agencia afectan a cómo ejercerlos.

Y, además, las tutelas de derechos solicitadas a la Agencia por los ciudadanos se han incrementado en un 88% en 2008.

¿Qué derechos son los que más preocupan a los ciudadanos?: Primero: saber quién tiene sus datos y cómo los ha obtenido (un 22 % de las tutelas afectaron al derecho de acceso) y, segundo, saber cómo cancelarlos (un 70% de las tutelas).

De lo que se desprenden dos conclusiones:

-Que los ciudadanos carecen de información o no son conscientes de los datos personales que facilitan.

-Que, cuando son conscientes, tratan de impedir la utilización de sus datos solicitando su cancelación.

Más tarde haré referencia al ejercicio de derechos relacionados con servicios en Internet, pero, de entrada, quiero apuntarles que las principales cuestiones sobre las que se ejercen los derechos de acceso y cancelación afectan:

- a la información sobre solvencia en ficheros de morosos, a la historia clínica y a las imágenes objeto de videovigilancia.

- a la cancelación de datos en ficheros de morosidad y en historias clínicas.

- y afectan, también, a las solicitudes de cancelación de datos que obran en poder de operadores de telecomunicaciones una vez concluida la prestación de los servicios contratados y a la supresión de antecedentes policiales, penales y penitenciarios.

Sobre el conjunto de estas reclamaciones quiero destacar un dato significativo:

- En 2008, las tutelas estimadas se han incrementado un 10% sobre 2007; año en que como informé ante esta Comisión, se estimaron un 80% de las reclamaciones.

Las principales causas de este incremento residen en:
- que los responsables de los ficheros ni siquiera contestaron a los ciudadanos,
- o que lo hicieron ya durante la tramitación del procedimiento administrativo iniciado por la Agencia (es decir, se detecta una cierta desidia que sólo desaparece cuando interviene la Agencia).

No obstante, quiero advertir a sus Señorías que estos datos de la Memoria de 2008 están condicionados por el importante volumen de ejercicio del derecho de cancelación en los libros registro de bautismo de la Iglesia católica.

Y, como ustedes conocen, la STS de 19 de septiembre de 2008 y sucesivas han venido a considerar que la LOPD no les resulta aplicable, como ya informé a la Comisión en mi última comparecencia.

***

Lo cierto es que la mejor forma de que los ciudadanos estén protegidos consiste en que quienes vayan a tratar sus datos lo hagan cumpliendo con las garantías de la Ley.

Lo que exige de la Agencia facilitar de la forma más fluida y sencilla el conocimiento y cumplimiento de las obligaciones.

Por ello, la Agencia atiende las dudas de los responsables de ficheros para ayudarles a resolver situaciones complejas propias de una actividad económica globalizada y cambiante como consecuencia del desarrollo tecnológico.

No debe olvidarse que la seguridad jurídica en la actividad económica es un factor que puede reducir costes organizativos, tecnológicos, de asesoramiento legal y de minimización de riesgos.

Las consultas más complejas atendidas por el Gabinete Jurídico de la Agencia se incrementaron en 2008 un 25% (60% en el sector privado y un 40% en el público).

Los principales sectores privados que han demandado el criterio de la Agencia son los de asesoría y consultoría, telecomunicaciones, servicios de la sociedad de la información y asociaciones profesionales y empresariales.

En particular, los sectores de las telecomunicaciones y de los servicios de la sociedad de la información plantean nuevos retos e interrogantes sobre la protección de datos personales que, en la medida de lo posible, intentamos abordar con las empresas en una relación fluida y próxima.

Las principales dudas planteadas estaban relacionadas en 2008 con la entrada en vigor del nuevo Reglamento de Protección de Datos, especialmente en materias tales como su ámbito de aplicación (por ejemplo, la exclusión de personas de contacto de todo tipo de organizaciones y empresarios autónomos), exigencias de información a los ciudadanos y cumplimiento de medidas de seguridad.

La actividad consultiva de la Agencia se ha traducido en la emisión de 79 informes preceptivos a disposiciones de carácter general.

Todos estos informes abarcan un amplio abanico de actividades como, por ejemplo, la Administración de Justicia; el control de los precursores de drogas; el Reglamento de conductores y los seguros obligatorios de automóviles, la interrupción voluntaria del embarazo; el “doping”, la violencia, el racismo, la xenofobia y la intolerancia en el deporte o la restitución a particulares de documentos incautados durante la guerra civil.

En conexión con el informe sobre el Reglamento de la Ley de Protección de la Salud y lucha contra el dopaje en el Deporte permítanme un inciso sobre la

intervención de la Agencia en la redacción del Estándar internacional para la protección de la privacidad y de la información personal de la Agencia Mundial Antidopaje. En dicho Estándar se ha planteado la necesidad de garantizar un equilibrio entre el tratamiento de la información precisa para la lucha contra el doping en el deporte y los derechos de los deportistas. En el proceso de negociación fomentado por el Consejo Superior de Deportes, la Agencia ha contribuido a incorporar mejoras para adaptarlo a los niveles de protección exigidos por la normativa española y comunitaria.

Pero para la mayor parte del tejido empresarial español, constituido por PYMES, la incidencia de las normas de protección de datos no se traduce en problemas jurídicos complejos.

Lo que necesitan y demandan es, lisa y llanamente, saber de una forma sencilla, comprensible y detallada qué tienen que hacer para cumplir la LOPD.
Para dar respuesta a esta necesidad, la AEPD ha editado diversas guías dirigidas a facilitar con un leguaje claro, sencillo y fácilmente comprensible los aspectos básicos de la protección de datos personales.

Por ejemplo, se han publicado la “Guía de Protección de datos para Responsables de ficheros” y la “Guía de seguridad de los datos”.

La respuesta a las iniciativas de concienciación, información y simplificación del cumplimiento por la Agencia se constata, al menos parcialmente, en el incremento de ficheros inscritos en el RGPD.

En 2008 se inscribieron más de 250.000 nuevos ficheros (incrementándose un 21%) cuyos titulares son, en su mayor parte, PYMES (principalmente en sectores como el comercio; la contabilidad, auditoria y asesoría fiscal, las actividades inmobiliarias y la construcción). A 1 de junio se han inscrito más de 166.000 nuevos ficheros en 2009 con lo que la cifra total se aproxima hoy al millón y medio.

En conclusión: el alcance del conocimiento y cumplimiento de la LOPD en nuestro tejido empresarial es irreversible.

Junto a ello debo destacar el incremento del 300% en el registro de ficheros de titularidad pública, con un peso muy importante de ficheros de la Administración de Justicia (casi 12.000); cuestión ésta a la que me referiré específicamente. A lo que se añade la inscripción de ficheros de otros Órganos tan relevantes como el propio Congreso de los Diputados, el Defensor del Pueblo y el Tribunal Constitucional

Los datos que he expuesto a sus Señorías indican, quiero insistir en ello, una tendencia consolidada de mayor conocimiento por los ciudadanos y más nivel de cumplimiento por los responsables de bases de datos.

Pero esta constatación no es óbice para que el número de denuncias por infracciones de la LOPD siga incrementándose. Trataré de ofrecerles, sintéticamente algunos indicadores ilustrativos referidos a 2008:

- las inspecciones crecieron en un 45 % y las resoluciones de procedimientos sancionadores casi se duplicaron (aumentaron un 94%)

- Los principales sectores afectados siguen siendo, como en las últimas Memorias, los de telecomunicaciones y entidades financieras. A los que, se añaden, como anticipé en mi anterior comparecencia, las actividades de videovigilancia, que comentaré posteriormente.

En particular, los procedimientos sancionadores en los sectores de telecomunicaciones y entidades financieras se han incrementado en porcentajes muy superiores al año anterior (81 y 59%, respectivamente).

Quisiera destacar como avance, que también en 2009 el número de reclamaciones, junto con la inspecciones de la Agencia, están protagonizando un crecimiento muy importante. A 1 de junio las denuncias se han incrementado en un 60% y las actuaciones posteriores en un 138%.

En 2008, las sanciones ascendieron a 22,6 millones de euros, con un incremento del 15% sobre el año anterior. Esta cifra se explica por el fuerte incremento del número de resoluciones sancionadoras (56%) pero está por debajo

de las sanciones declaradas en 2006 que casi alcanzaron los 24,5 millones de euros.

Contribuyen a explicar esta reducción relativa del volumen total de multas:

- Por un lado, la estabilidad de las infracciones graves (las más habituales) y leves.
- Y, por otro, la apreciación de circunstancias que disminuyen cualificadamente la responsabilidad (en un 42% del total de resoluciones sancionadoras; un 10 % más que en 2007).

Por su parte, las resoluciones de archivo y las denuncias inadmitidas aumentaron en un 113% y 138,3% respectivamente.

En cuanto a las infracciones cometidas por las Administraciones Públicas destaca un incremento cercano al 20% - que resulta mayor en las Administraciones Autonómicas (31%) que en la local (14%); descendiendo en la Administración General del Estado (-4,5%).

De las infracciones declaradas a Administraciones Públicas debo llamar la atención a las referidas:

- al hallazgo de documentación en la vía pública.
- A la publicación en webs corporativas de datos facilitados por los ciudadanos.

Para finalizar la primera parte de mi intervención, haré referencia a algunos datos sobre en qué medida los Tribunales (Audiencia Nacional y Tribunal Supremo) han ratificado los criterios de la AEPD y, con ello, sobre el nivel de seguridad jurídica que proporcionan las resoluciones de la Agencia en la aplicación de la Ley.

- Un 72 % de las sentencias de la AN confirman las resoluciones de la Agencia.
- Un 6% de las sentencias estimaron parcialmente los recursos interpuestos en la mayor parte de los casos modificando la cuantía de la sanción.
- Un 21% de las sentencias estimaron las pretensiones anulatorias de las resoluciones de la AEPD. Aunque casi la mitad de ellas (22 sentencias sobre 48)

afectaban a los Libros de Bautismo y asumían el criterio de la STS de 19 de septiembre de 2008.

Por su parte, el Tribunal Supremo ratificó en todos los casos las sentencias que confirmaban las resoluciones de la AEPD, excepto las relativas a los libros de bautismo.

***

La segunda parte de mi intervención la dedicaré a informar a la Comisión sobre los que, a mi juicio, son los principales retos e interrogantes que se están planteando para la privacidad en la actualidad.

Comenzaré refiriéndome a una cuestión que está directamente vinculada con la última información que les he facilitado sobre la Memoria 2008, en relación con la Administración de Justicia.

En mi anterior comparecencia trasladé a la Comisión la preocupación de la Agencia sobre el cumplimiento de la LOPD en la Administración de Justicia. Informé a Sus Señorías sobre las inspecciones realizadas a órganos judiciales cuya documentación había sido encontrada en contenedores de basura cercanos a sus sedes. Unos hechos inaceptables y más aún tratándose de datos aún de datos de naturaleza sensible.

Además, compartí con la Comisión la propuesta de creación de un órgano de trabajo con el CGPJ, el Ministerio de Justicia y las Comunidades Autónomas dirigido a mejorar el cumplimiento de la normativa de protección de datos.

En 2008 se han constatado algunos avances en este ámbito.

En primer lugar, el CGPJ ha llevado a cabo una inscripción masiva de los ficheros vinculados a los órganos judiciales (casi 12.000). Su importancia radica en que nos permite conocer qué ficheros tienen naturaleza jurisdiccional o gubernativa y quienes son sus responsables (el titular del órgano, el secretario, el Ministerio de Justicia o las Comunidades Autónomas). Además, nos ayuda a conocer a qué instancias corresponde implantar las medidas de seguridad que deben impedir el

abandono de la documentación judicial en la vía pública. (Comunidades Autónomas y Ministerio de Justicia).

En las inspecciones realizadas se constató qué órganos judiciales, en el ejercicio de su responsabilidad, han demandado, pero no han obtenido de las Administraciones Autonómicas, respuesta sobre la implantación de medidas de seguridad. Diligencia ésta que, lamentablemente, no ha existido en otros casos.

Por ello, tal y como se ha podido conocer en los últimos días, la Agencia ha iniciado recientemente procedimientos por infracción de la LOPD a cinco órganos judiciales de Madrid, Valencia, Sevilla y Galicia y a las Consejerías de Justicia de Valencia, Galicia y Andalucía.

Junto a ello, se ha dado traslado de las actuaciones practicadas a las Agencias de Protección de Datos de Madrid y Cataluña por si procede iniciar actuaciones contra sus respectivas Consejerías de Justicia.

En segundo lugar, la Agencia ha intercambiado criterios con el CGPJ sobre cómo deben coordinarse en el ejercicio de sus respectivas competencias de inspección; aspecto que constituye un presupuesto previo para evaluar el cumplimiento de la LOPD en los órganos judiciales.

Por ello, puede realizarse una valoración positiva pues se han articulado unas bases sólidas para resolver esta cuestión.

La Agencia propondrá, en este año, una iniciativa a los Poderes y Administraciones implicadas para la constitución de un órgano de trabajo que permita impulsar el objetivo que les he señalado.

El segundo de los retos es el de la videovigilancia. La Memoria de 2008 ratifica una conclusión que he ido anticipando en mis anteriores comparecencias: El incremento de la videovigilancia es un fenómeno imparable que exige garantizar un punto de equilibrio entre las necesidades de videovigilancia por razones de seguridad y la protección de la privacidad y de los datos personales.

Los datos de 2008 son significativos:

- Los ficheros de videovigilancia inscritos en el Registro de la Agencia se duplicaron en 2008 alcanzando la cifra de 15.510. Y A 1 de junio de 2009 son casi 25.000.
- El 98% de los ficheros son privados, alcanzando su mayor implantación en el comercio, turismo y hostelería y comunidades de propietarios.
- Un fenómeno que nos preocupa especialmente consiste en que en el sector educativo estamos asistiendo a un crecimiento exponencial de ficheros de videovigilancia (que en 2008 fue ya del 270%).

Esta tendencia se mantiene en 2009 con un crecimiento del 58% (siendo casi 400 los ficheros de videovigilancia inscritos). Muchas de estas inscripciones son iniciativas autónomas de los centros educativos sin la intervención de las respectivas Consejerías de Educación que deben dictar las disposiciones para su creación. De ahí que la Agencia se ha dirigido a algunas de ellas para que regularicen la situación.

- Además, debo resaltar que las inspecciones sobre videovigilancia suponen el 15% del total de las realizadas y las resoluciones sancionadoras se incrementaron en 2008 en más de un 600%.

En mi última comparecencia ya informé a sus Señorías sobre la percepción de los ciudadanos acerca de este fenómeno y hoy lo haré sobre las iniciativas de la Agencia respecto de la videovigilancia.

La primera prioridad ha sido de naturaleza informativa y preventiva. Los datos indican que los mayores incrementos de la videovigilancia tienen lugar en el sector privado y, en particular, en sectores donde se constata un gran peso de las PYMES y, también, en las comunidades de propietarios.

Pero existe un fuerte déficit de información. Por ello, la Agencia ha publicado en una “Guía de videovigilancia” que expone de forma clara y comprensible cómo puede desarrollarse esta actividad garantizando los derechos de los ciudadanos.

Además, hemos tramitado 44 procedimientos sancionadores relacionados con la videovigilancia que suponen un incremento de 600% sobre el año anterior.

También hemos ampliado el análisis sobre el uso de cámaras a otras actividades que no siempre tienen como objetivo la seguridad y que según hemos podido constatar, plantean importantes riesgos para la privacidad e incluso para la propia seguridad: es el caso de las videocámaras en Internet. Se trata de cámaras de video conectadas a Internet que permiten un acceso remoto a través de la Red al visionado de las imágenes en tiempo real.

El uso de cámaras de video se ha extendido de forma generalizada en los últimos años, a medida que su coste ha disminuido progresivamente hasta convertirse en dispositivos al alcance de gran público.
De cámaras pensadas inicialmente para formar partes de circuitos cerrados de televisión muy localizados se ha pasado a las webcams capaces de conectarse directamente a redes públicas con alcance global.

La tecnología permite incluir en una única conexión todas las funcionalidades disponibles de la cámara: video, sonido, control de movimiento.

E, inicialmente utilizadas con fines básicamente de seguridad, han surgido otros como el control de la actividad laboral y la genérica difusión de una actividad de un determinado espacio (abierto o cerrado, público o privado).

Teniendo en cuenta la fuerte expansión que están teniendo las video cámaras en Internet y el potencial impacto que para la privacidad presentan estos dispositivos, la Agencia ha concluido una inspección general de oficio cuyas conclusiones básicas puedo anticipar a la Comisión:

- Parte importante de las cámaras detectadas recogen imágenes de la vía pública, el lugar de trabajo o del interior de establecimientos comerciales.

- Se difunden las imágenes en abierto, es decir, sin ningún tipo de control de acceso, lo que deriva en una situación de elevado impacto para la privacidad.

_ Obviamente, las imágenes captadas en la vía publica suponen un grave incumplimiento que reserva dicha facultad a las Fuerzas y Cuerpos de Seguridad.

También en el ámbito laboral el desarrollo tecnológico y de nuevas modalidades de control está condicionando las garantías de privacidad de los trabajadores.

La integración de datos biométricos para el control horario, el acceso al correo electrónico que usan los trabajadores, la instalación de videocámaras y grabación de voz por razones de seguridad, la geolocalización, el acceso a información médica sin garantías o la implantación creciente de sistemas de denuncia interna y anónima de las empresas, son indicativos de este riesgo.

Para alcanzar soluciones de equilibrio dentro de un enfoque global hemos incluido en esta Memoria una recomendación dirigida a promover espacios de concertación social que permitan la protección integral de los datos personales en el entorno laboral.

En el marco de las inspecciones sectoriales de la Agencia, ya informé a la Comisión sobre la iniciación de una nueva inspección sobre llamadas telefónicas no solicitadas con fines comerciales y mensajes publicitarios a teléfonos móviles.

En la anterior comparecencia llamé la atención sobre la necesidad de poner límite al acoso al que se ven sometidos los ciudadanos a través de estos canales publicitarios, hoy les resumiré las conclusiones más relevantes de esta inspección:

Todos nos hemos preguntado alguna vez: ¿de donde se obtienen nuestros datos para hacer publicidad telefónica?.

El ciudadano cree estar indefenso ante el acoso al que se ve sometido con constantes llamadas y mensajes publicitarios. Y lo cierto es que, aunque existen algunas vías de defensa, también hay importantes deficiencias en los mecanismos para hacer frente esta intrusión en la vida de los ciudadanos.

Los resultados de la inspección ponen de manifiesto lo siguiente:

-En torno al 30% de los operadores realizan la publicidad dirigida a sus clientes o a los de otras empresas del mismo grupo empresarial con su consentimiento, obtenido en el momento de la contratación.

- También se dirigen campañas publicitarias a terceros no clientes, cuyos datos se han obtenido por empresas especializadas de fuentes accesibles al público o con el consentimiento de los interesados.

- Una tercera técnica, menos extendida, es la de realizar llamadas publicitarias a terceras personas “recomendadas” por los propios clientes. Esta opción exige contar con el consentimiento de los “recomendados”, por lo que la Agencia ha sancionado ya a las empresas que promueven la campaña y no a quienes los recomendaron.

- En la publicidad a través del teléfono fijo los datos utilizados proceden fundamentalmente de la edición electrónica de las guías telefónicas.

De este modo, se excluyen de la compaña publicitaria a los abonados que no figuran en la guía o que figurando, se oponen al uso de los datos con fines publicitarios.

- En la publicidad a través de telefonía móvil constituye práctica habitual, ante la inexistencia de guías, seleccionar aleatoriamente los números de teléfono, atendiendo a los rangos de numeración móvil asignados a otros operadores.

Ante este escenario, ¿Qué podemos hacer para evitar el acoso publicitario a través de llamadas telefónicas?

La primera opción es el derecho a no figurar en la guía o a figurar indicando que los datos no pueden ser utilizados con fines publicitarios.

Esta opción es eficaz frente a las llamadas a teléfonos fijos pero no frente a llamadas aleatorias a móviles donde, reitero, las guías telefónicas son inexistentes.

Sin embargo, la proporción de abonados cuyos datos se publican en guías es bastante superior al 75%.

Y, tan solo el 1% han solicitado que sus datos se marquen para impedir su uso publicitario.

De lo que se desprende: o que los ciudadanos no son demasiado reticentes a estas actividades; o que, más bien, no son conscientes de este derecho.

La segunda opción para evitar este fenómeno la contempla el Reglamento de Protección de Datos: impulsar los “ficheros de exclusión”, en los que se incluyen los abonados o usuarios que se han manifestado en contra de la recepción de publicidad.

La práctica totalidad de las compañías encuestadas filtran los destinatarios de las campañas publicitarias con sus propios ficheros de exclusión.

Pero, los ficheros de autoexclusión hoy existentes tienen una eficacia limitada pues están dirigidos básicamente a impedir comunicaciones publicitarias a través del correo postal.

Para impulsar un Fichero de Autoexclusión que pueda ser un instrumento eficaz para los ciudadanos que no desean recibir publicidad, la Agencia y la Federación Española de Marketing Directo estamos impulsando iniciativas que permitan garantizar este derecho de autoexclusión.

Sin embargo cuando la publicidad a través de llamadas telefónicas realizadas a través de operadora no está asociada a datos personales existe un vacío legal pues la Ley General de Telecomunicaciones no ha contemplado una infracción específica.

Por ello, la Memoria de 2008 incluye una recomendación que permita cubrir este vacío legal.

En cuanto a la inspección sectorial sobre mensajes publicitarios y comerciales a telefonía móvil se ha detectado:

- La falta de claridad en la información que se facilita a los clientes.
- El envío masivo de mensajes SMS con publicidad realizados por empresas que no tienen relación comercial previa con quienes los reciben.
- La realización de altas sin informar al usuario de que se trata de servicios de tarificación adicional. Deficiencia sobre la que debe alertarse, especialmente, cuando la suscripción la realizan menores de edad.

Pero los mayores retos que hoy se nos plantean, a quienes tenemos encomendada la tarea de proteger de la privacidad de los ciudadanos, siguen centrados en Internet, (especialmente para los usuarios menores de edad). Y ello a causa, fundamentalmente:

- del dinamismo en la oferta de estos nuevos servicios.
- y de que dichos servicios de Internet se prestan por entidades establecidas en terceros países pero se dirigen a usuarios de cualquier lugar del mundo.

En anteriores comparecencias he ido informando a la Comisión sobre el mal uso de programas de intercambio de archivos (eMule) que dan lugar a la difusión de datos personales en Internet, por un gravísimo problema de desconocimiento e ignorancia en el uso de estas tecnologías de Internet.

La Agencia ha resuelto un total de 28 procedimientos declarando infracciones de la LOPD. Pero para apreciar la gravedad de estas conductas no bastan los meros datos cuantitativos sino otras circunstancias como las siguientes:

- Entre los datos que se difunden involuntariamente hay datos muy sensibles como son los de salud, de ideología y afiliación sindical.

- Entre los infractores se encuentran entidades a las que cabe exigir una sensibilidad cualificada sobre la privacidad como partidos políticos y sindicatos.

- Y, también, las propias Administraciones públicas, han permitido la difusión de datos de ciudadanos por el mal uso que hacen sus propios empleados públicos de programas de intercambio de archivos.

Sobre la difusión de imágenes en portales de Internet como “You Tube” quiero reseñar que la Agencia ha resuelto ya tres procedimientos sancionadores e impuesto las correspondientes sanciones.

Estas resoluciones ponen de manifiesto la importancia de que los ciudadanos sean concientes y asuman su responsabilidad en el entorno del Internet interactivo ante difusión de información personal (datos, fotografías y videos) propios y de terceros.

Sin perjuicio de ello, la Agencia está incentivando que los ciudadanos ejerciten directamente el derecho de cancelación ante los responsables de los portales de Internet en que se difunden imágenes u otra información personal.

Se pretende así limitar en el tiempo la difusión de las imágenes y la intromisión que implica para su titular.

Como conocen Sus Señorías, uno de los efectos del desarrollo de los motores de búsqueda de Internet ha sido la multiplicación universal de las posibilidades de acceder a las informaciones publicadas en Diarios y Boletines Oficiales.

Basta con teclear en un buscador el nombre y apellidos de alguien para que cualquier persona pueda conocer si se ha tenido alguna incidencia sobre infracciones administrativas, si ha podido cometer un delito del que ha sido indultado, si tiene problemas con el consumo de drogas o si su solvencia económica está en entredicho por existir procedimientos administrativos o judiciales sobre posibles deudas pendientes.

Esta información puede afectar a la consideración de los alumnos sobre sus educadores, a la de los hijos sobre los padres, a la actividad profesional de los ciudadanos o, en general, a la valoración que perciba su entorno social.

Un número creciente de ciudadanos han reaccionado reclamando su derecho al olvido en Internet.

Así lo afirma el Defensor del Pueblo que en su Informe de 2008 hace referencia a un número especialmente significativo de quejas sobre esta materia y, al tiempo nos recuerda que, si bien la publicación de la información está amparada por las leyes procedimentales y no depende del consentimiento de los interesados, cuando estas normas “contemplan la publicación de determinados actos o trámites (…) no preveían ni pretendían la multiplicación y permanencia en el tiempo de dicha publicación (…), de la que pueden derivarse resultados que afectarían a la integridad del derecho a la protección de datos, en los términos en que ha sido definido por el Tribunal Constitucional”.

Por ello, el Defensor del Pueblo ha demandado de la Agencia información sobre las soluciones “normativas o de otra índole” que puedan adoptarse.

La Agencia ha recibido, también, numerosas reclamaciones al respecto.

Por ello, hemos tomado la iniciativa que anticipé en mi anterior comparecencia para dar una respuesta global a estas inquietudes.

Tras un amplio proceso de consultas, estamos ultimando un proyecto de Instrucción sobre la publicación de información personal en diarios y boletines oficiales que pretende:

- Primero.- Minimizar los datos personales que se publican, sin afectar a los fines legales de la publicación.
- Segundo.- Ofrecer mecanismos para que sean los interesados los que accedan al contenido íntegro de los actos administrativos.
- Tercero.- Ordenar los procedimientos de ejercicio de los derechos de protección de datos.
- Cuarto.- Evitar la indexación por parte de los motores de búsqueda de la información publicada, cuando lesionen los derechos individuales, según la tecnología disponible.

Con esta iniciativa pretendemos dar cumplimiento a la recomendación formulada en la Memoria 2007.

Sin embargo, el principal interrogante recogido en la Memoria 2008 y plenamente vivo en la actualidad se cierne sobre las Redes Sociales de Internet ante el importante impacto en la privacidad de sus millones de usuarios.

Las redes sociales on line son servicios que permiten a los usuarios generar un perfil público en el que plasmar datos personales, con la posibilidad de interactuar con otros usuarios afines o no al perfil publicado. También permite el intercambio de información de terceros no usuarios como, por ejemplo, imágenes.

La Agencia, anticipándose a las reclamaciones de los ciudadanos, tomó la iniciativa en 2008 de analizar la incidencia que pudieran tener sobre la privacidad y la seguridad de la información a través de un estudio conjunto con el Instituto Nacional de Tecnologías de la Información.

Del estudio se desprende que los principales elementos de riesgo en relación con la información personal son:

- Las carencias en las políticas de privacidad y condiciones de uso por:
    - Estar alojados en lugares del sitio web de difícil acceso.
    - Resultar confusas y prolijas.
    - Ser de difícil comprensión para un usuario medio que no disponga de conocimientos jurídicos y tecnológicos.

Los déficits de información dificultan la toma de conciencia real por los usuarios sobre quienes podrán acceder a sus perfiles. Casi la mitad de los usuarios de redes sociales analizados tienen su perfil de usuario sin restricciones de la privacidad y pueden ser vistos por cualquier persona. Una situación que provoca no poco riesgos para la privacidad de los usuarios.

Riesgos confirmados por noticias referidas a la utilización de la redes sociales, en determinados países, para la obtención de información y la posterior comisión de secuestros, por la posibilidad de suplantación de identidad, o incluso a por

situaciones tales como despidos laborales por comentarios vertidos en estas redes sociales.

Este estudio analiza los riesgos para la privacidad en las fases de registro del usuario, cuando utiliza la red social y al darse de baja en el servicio y concluye lo que sigue:

- que resultan excesivos los datos solicitados en el formulario de registro (por ejemplo, de ideología política, orientación sexual y preferencia religiosa). Estos datos serán visibles por todos sus contactos y, dependiendo de la configuración del perfil, por todos los usuarios de la red.
- que el grado de publicidad del perfil de usuario resulta demasiado elevado.
- que se publica información personal propia y de terceros que no han prestado el consentimiento para ello.
- que no es extraña la suplantación de identidad de los usuarios de la red social.
- que el perfil de usuario es, en ocasiones, indexado automáticamente por los buscadores en Internet.
- que se promueve la recepción de comunicaciones comerciales electrónicas no solicitadas.
- que se dificulta la baja efectiva del servicio manteniendo los datos a disposición de los responsables de la red.

Además, quiero hacer una referencia destacada a la protección de la privacidad de menores y adolescentes.

El estudio realizado indica que un 36,5% de los usuarios de redes sociales tienen entre 15 y 24 años. De ellos, todos los menores de entre 14 y 16 años son usuarios habituales y publican información personal y familiar.

Hay que añadir que los menores de 14 años acceden a estos servicios a pesar de que nuestra normativa establece que el tratamiento de los datos de los menores de 14 años exige del consentimiento de sus padres o representantes legales.
El estudio constata que los responsables de redes sociales no han implantado mecanismos eficaces de comprobación de la edad.

Además, los menores de edad están expuestos a riesgos específicos en las redes sociales, como son:

- El acceso a contenidos inapropiados para su edad.
- La posibilidad de entablar contacto con usuarios malintencionados.
- O a la proliferación de información personal y gráfica publicada por ellos mismos o por terceros con desconocimiento de los riesgos asociados.

Por si fuera poco, hay que tener en cuenta que:

- El 77% de los menores que utilizan redes sociales tienen visible su perfil público.
- Otros estudios evidencian que el 52% de las víctimas de ciberbullying tiene entre 13 y 14 años (el 10% no ha cumplido los 10 años) y el 60% son niñas. Las víctimas sufren ciberbullying a través de webs, foros, redes sociales y del Messenger (45%); por correo electrónico (12%) o a través del teléfono móvil (19%).

Para abordar estos riesgos hay que partir de la premisa de que los menores y adolescentes son “nativos digitales” y contestar las siguientes preguntas:
¿Conocen los padres las actividades de sus hijos en Internet y, en particular en las redes sociales?
¿Tienen información sobre las medidas de control parental que tienen a su disposición?
¿Conocen los educadores estos riesgos y están capacitados para formar a estos “nativos digitales” sobre un uso consciente de estos servicios?
¿Conocen los propios usuarios menores y adolescentes estos riesgos y sus posibles consecuencias presentes o futuras?

Creo que coincidirán conmigo en que, con carácter general, la respuesta es negativa.

La protección de nuestros menores es una preocupación primordial de toda sociedad, y también de la Agencia. Por ello, estamos evaluando a las principales

redes sociales (como Tuenti o Facebook) para mejorar la aplicación de la normativa de protección de datos a estos servicios.
Buscamos que se implanten medidas eficaces para controlar la edad de los menores y excluir como usuarios a quienes tengan menos de 14 años (a lo que, de hecho, ya se ha comprometido con la Agencia una de las principales redes sociales existentes en nuestro país).

Esta preocupación es compartida por otras instituciones.

Así, la Comisaria europea responsable de los servicios de la sociedad de la información y medios de comunicación, ha alcanzado un compromiso en términos similares con 17 de los principales responsables de redes sociales.
Y el Defensor del Pueblo, ante quejas de ciudadanos por la inexistencia de control sobre las redes sociales, ha solicitado de la Agencia información al respecto.

Esta misma semana el Grupo de autoridades de protección de datos de todos los Estados miembros de la Unión Europea ha aprobado un Dictamen relativo a las redes sociales online en el que formula recomendaciones a los proveedores de redes sociales dirigidas a fortalecer los derechos de los usuarios.

Teniendo en cuenta la amplia acogida que tienen las redes sociales entre niños y jóvenes, la concienciación es uno de los pilares claves para asegurar una participación activa de los menores en cuanto al buen uso de estas redes.

Permítanme que les insista sobre la trascendencia del tema a la vista de las denuncias interpuestas ante la Agencia. Los afectados han empezado a reclamar la intervención de la Agencia a través de 19 denuncias (en su mayor parte referidas a la difusión de imágenes o documentos con datos de terceros sin su consentimiento (18) y a la suplantación de identidad (1)).

Asimismo, puedo anunciar que la Agencia, de oficio, ha iniciado inspecciones referidas a sitios web de contactos como VOTAMICUERPO que prestan servicios al público en general sin contar con garantías para los menores de edad; difundiéndose sin restricciones fotografías de jóvenes que, en una proporción importante, sugieren una edad menor de 14 años.

La ausencia de controles específicos en este tipo de servicios posibilitan el contacto directo (a través de correo electrónico, mensajería instantánea o incluso teléfono) con menores, favoreciendo la comisión de delitos relacionados con el acoso sexual. Muestra de ello, son sin duda las informaciones conocidas este último fin de semana relativas a la detención en España de un Ciberacosador que chantajeaba a más de 250 victimas, tras convencerlas para que le enviaran vídeos y fotos.

La Agencia ha tomado iniciativas de concienciación como la publicación, en el día de Internet, de una “Guía sobre derechos de los niños y niñas y deberes de padres y madres”. En ella se incorporan recomendaciones básicas para concienciar sobre la importancia de la protección de datos en el entorno de la familia y la escuela.

Sin embargo, estas iniciativas, aún teniendo una buena acogida, no son suficientes.

En la Memoria de 2007 ya se incluyó una recomendación que requería una actuación decidida de los poderes públicos dirigida a la protección de los menores en Internet.

Pero es preciso ir más allá. En el último debate sobre el Estado de la Nación esta Cámara ha adoptado una resolución en la que se insta al Gobierno en colaboración con la comunidad educativa y las Comunidades Autónomas, a apostar por la modernización e innovación de nuestro sistema educativo generalizando la incorporación de las tecnologías de la información y la comunicación a los sistemas de enseñanza y aprendizaje; extendiendo la dotación de ordenadores al alumnado de los últimos cursos de Primaria y de Secundaria; favoreciendo el trabajo en red entre los centros educativos y la comunidad educativa, así como la formación del profesorado.

No puede por menos que aplaudirse esta iniciativa. Pero creo que en ella debe atenderse, también, el conocimiento y la formación sobre la protección de datos personales y la privacidad ante las nuevas tecnologías.

Como pueden ver Sus Señorías, el uso de servicios en Internet presenta aspectos complejos.

Por ello quiero someter a la reflexión de los Grupos Parlamentarios la oportunidad de constituir un espacio parlamentario de análisis y reflexión en el que puedan evaluarse las múltiples problemáticas generadas por la revolución tecnológica que se ciernen sobre la privacidad de los ciudadanos.

E insistir en la recomendación que ya formulamos a los medios de comunicación para que, a través de la propia autorregulación se alcance un desarrollo de buenas prácticas en materia de privacidad.

El acceso y la difusión general por los medios de informaciones privadas de menores obtenidas de redes sociales, cuando son objeto de interés informativo, acentúan la vigencia de esta recomendación: El caso de la joven Marta del Castillo no requiere comentarios adicionales.

***

Terminaré esta intervención haciendo referencia a la actividad internacional de la Agencia y, en particular a dos temas de especial importancia.

El pasado año ya anunciaba a Sus Señorías que la Agencia presentaría su candidatura para optar a la organización de la Conferencia Internacional de Autoridades de Protección de Datos y Privacidad de este año 2009. Nuestra propuesta fue unánimemente aceptada, y así, el próximo mes de noviembre Madrid será sede de la 31ª Conferencia Internacional.

Para que puedan tener una idea aproximada del alcance de este evento que constituye el mayor foro de la privacidad a nivel mundial, destacaré tan sólo que contará con la asistencia de más de mil participantes, entre ellos los representantes de más de 80 autoridades de protección de datos de los cinco continentes y de las principales compañías mundiales de tecnología.

El tema central de la Conferencia será el impacto presente y futuro de las nuevas tecnologías de la información y la comunicación en el derecho a la protección de datos. Como su lema apunta (“privacidad: hoy es mañana”) nuestra intención es que los debates partan de la idea de que el desarrollo de estas tecnologías es imparable y acelerado, y que si queremos que se realice de un modo respetuoso con el derecho de los ciudadanos a la protección de su información personal, debemos trabajar desde hoy mismo, anticipándonos a esa evolución.

El segundo asunto sobre el que querría llamar la atención de Sus Señorías está también relacionado con la Conferencia.

En su última edición, celebrada en Estrasburgo, la Agencia presentó, conjuntamente con su homóloga suiza, una propuesta de resolución cuyo objetivo era que la Conferencia iniciara los trabajos para la redacción de unos estándares internacionales de protección de datos. Esta iniciativa partía de la constatación de que las diferencias entre los sistemas de protección de la información personal y la privacidad existentes en las diversas regiones del mundo suponen un obstáculo para los intercambios económicos y pueden conducir a situaciones de menor nivel de protección.

La propuesta española recibió un amplísimo respaldo y la Agencia recibió el mandato de liderar un proceso de elaboración que debe culminar con la presentación de un texto a la Conferencia de Madrid.

Con este fin, hemos convocado, y estamos coordinando, un grupo de trabajo formado por cerca de 30 autoridades de protección de datos que han querido unirse a este proyecto.

En cuanto a la Red Iberoamericana de Protección de datos hay que destacar que se ha consolidado la presencia institucional de países y ampliado el número de estos y que en el marco de sus actividades se ha fomentado un intercambio fluido de información con entidades privadas y con Autoridades de EEUU y europeas.
Para promover la incardinación de la red en la 31 Conferencia Internacional celebraremos la víspera a su inauguración en Madrid el VI Encuentro Iberoamericano de Protección de datos.

No quiero finalizar mi intervención sin una valoración positiva de los espacios de coordinación con las Agencias Autonómicas de Protección de Datos en la que destacan los intercambios en materia de videovigilancia, publicación de información en diarios y boletines oficiales e impulso a la educación de los menores.

Señor Presidente, Señorías. Uno de los aspectos inherentes a cualquier política pública es hacer frente a la indiferencia. Evitar que la repetición de un problema haga que nos acomodemos al mismo hasta convertirlo en crónico.

Al igual que en mi última comparecencia, quiero concluir con algunos titulares que nos recuerdan la enorme tarea pendiente.

El caso Marta del Castillo desvela riesgos para los menores en las redes sociales; La Fiscalía de Menores de Granada ordena quitar el perfil de una menor creado por otra persona para vejarla en una web para hacer amigos; El 20% de los casos de acoso escolar se producen en Internet; El maltrato a los profesores salta de las aulas a Internet; Empresas 'roban' datos a cerca de 190.000 niños en los colegios de Madrid; Facebook se reserva el derecho a controlar los contenidos de sus usuarios de forma perpetua y mundial; El escáner corporal que permite ver el cuerpo desnudo, y que ya funciona en algún aeropuerto de Europa, podría atentar contra los derechos fundamentales de los pasajeros; La Interpol quiere crear una base de datos de reconocimiento facial; Asociaciones británicas piden el cierre de Google Street View ; La desaparición de datos íntimos pone en jaque al Ejército británico; Roban los datos personales de 4,5 millones de demandantes de empleo británicos de Monster; Reino Unido planea una gran base de datos para las llamadas telefónicas y los emails; Roban un portátil con fotos íntimas de la familia real británica; Media Europa se enfrenta a Google por el derecho a la intimidad del ciudadano: el servicio panorámico de ciudades creado por el buscador no gusta en Alemania o Suiza; Un banco de Nueva York pierde datos personales de 12'5 millones de clientes; -Roban el ordenador de un investigador estadounidense con los datos médicos de 2.500 pacientes; El Archivo Nacional de EEUU pierde un disco duro con datos personales de empleados de la Casa Blanca en la era Clinton.

Confío en que la información que les he aportado haya sido de su interés y quedo a partir de este momento, Señor Presidente a disposición de la Comisión.